(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 898 425 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
24.02.1999 Bulletin 1999/08

(51) Int Cl.[6]: **H04N 7/167**, H04N 7/16

(21) Application number: **98306196.1**

(22) Date of filing: **04.08.1998**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **15.08.1997 US 911650**

(71) Applicant: **LUCENT TECHNOLOGIES INC.**
Murray Hill, New Jersey 07974-0636 (US)

(72) Inventor: **Wool, Avishai**
Livingston, New Jersey 07039 (US)

(74) Representative:
Watts, Christopher Malcolm Kelway, Dr.
Lucent Technologies (UK) Ltd,
5 Mornington Road
Woodford Green Essex, IG8 0TU (GB)

(54) Cryptographic method and apparatus for restricting access to transmitted programming content using extended headers

(57) A system for restricting access to transmitted programming content is disclosed, which transmits the encryption key used to encrypt the program to the customer with the encrypted programming content. A set-top terminal or similar mechanism restricts access to the transmitted multimedia information using stored decryption keys. The set-top terminal preferably receives one or more package keys, SJ, periodically from the service provider, each corresponding to a package of programs that the customer is entitled to for a given period. Each program is preferably encrypted by the head-end server pnor to transmission using a program key, KP, which may be unique to the program. Header information is transmitted with the encrypted program to the customers, containing a package pair for each package to which the program belongs. A package pair preferably includes an identifier of the package, as well as the program key, KP, encrypted by the corresponding package key, SJ. The broadcast of a given program, p, preferably consists of a header portion containing a package pair for each package that the program belongs to, and a program portion containing the program encrypted with the program key, KP. If a customer is entitled to a particular program, the set-top terminal will be able to decrypt the encrypted program key, KP, using an appropriate stored package key, SJ, and thereafter use the program key, KP, to decrypt the encrypted program. The header information can be interleaved with the program portion or transmitted on a separate dedicated control channel.

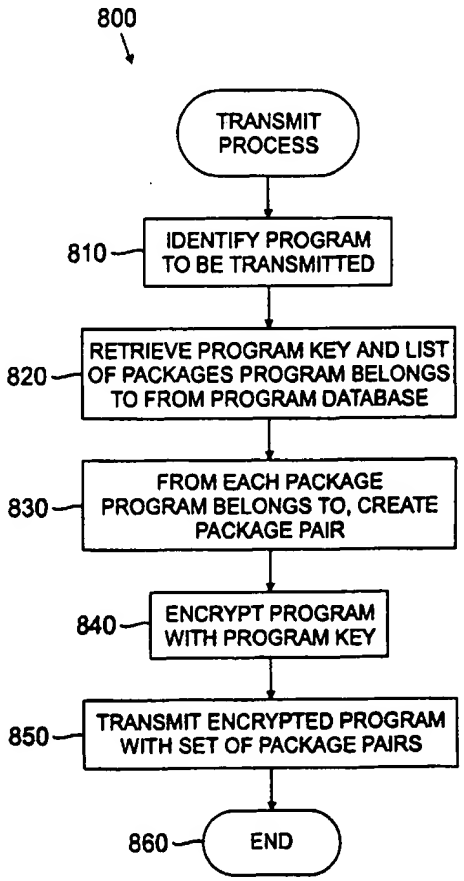

FIG. 8

EP 0 898 425 A2

Description

FIELD OF THE INVENTION

[0001] The present invention relates generally to a system for restricting access to transmitted programming content, and more particularly, to a system for transmitting an encrypted program together with the encryption key used to encrypt the program.

BACKGROUND OF THE INVENTION

[0002] As the number of channels available to television viewers has increased, along with the diversity of the programming content available on such channels, it has become increasingly challenging for service providers, such as cable television operators and digital satellite service operators, to offer packages of channels and programs that satisfy the majority of the television viewing population. The development of packages that may be offered to customers is generally a marketing function. Generally, a service provider desires to offer packages of various sizes, from a single program to all the programs, and various combinations in between.

[0003] The service provider typically broadcasts the television programs from a transmitter, often referred to as the "head-end," to a large population of customers. Each customer is typically entitled only to a subset of the received programming, associated with purchased packages. In a wireless broadcast environment, for example, the transmitted programming can be received by anyone with an appropriate receiver, such as an antenna or a satellite dish. Thus, in order to restrict access to a transmitted program to authorized customers who have purchased the required package, the service provider typically encrypts the transmitted programs and provides the customer with a set-top terminal (STT) containing one or more decryption keys which may be utilized to decrypt programs that a customer is entitled to. In this manner, the set-top terminal receives encrypted transmissions and decrypts the programs that the customer is entitled to, but nothing else.

[0004] In order to minimize piracy of the highly sensitive information stored in the set-top terminals, including the stored decryption keys, the set-top terminals typically contain a secure processor and secure memory, typically having a capacity on the order of a few kilobits, to store the decryption keys . The secure memory is generally non-volatile, and tamper-resistant. In addition, the secure memory is preferably writable, so that the keys may be reprogrammed as desired, for example, for each billing period. The limited secure memory capacity of conventional set-top terminals limits the number of keys that may be stored and thereby limits the number of packages which may be offered by a service provider. It is noted that the number of programs typically broadcast by a service provider during a monthly billing period can be on the order of 200,000.

[0005] In one variation, conventional set-top terminals contain a bit vector having a bit entry corresponding to each package of programs offered by the service provider. Typically, each package corresponds to one television channel. If a particular customer is entitled to a package, the corresponding bit entry in the bit vector stored in the set-top terminal is set to one ("1"). Thereafter, all programs transmitted by the service provider are encrypted with a single key. Upon receipt of a given program, the set-top terminal accesses the bit vector to determine if the corresponding bit entry has been set. If the bit entry has been set, the set-top terminal utilizes a single stored decryption key to decrypt the program.

[0006] While, in theory, flexibility is achieved in the bit vector scheme by providing a bit entry for each program, the length of the bit vector would be impractical in a system transmitting many programs in a single billing period. In addition, access control in such a system is provided exclusively by the entries in the bit vector and is not cryptographic. Thus, if a customer is able to overwrite the bit vector, and set all bits to one ("1"), then the customer obtains access to all programs.

[0007] In a further variation, programs are divided into packages, and all programs in a given package are encrypted using the same key. Again, each package typically corresponds to one television channel. The set-top terminal stores a decryption key for each package the customer is entitled to. Thus, if a program is to be included in a plurality of packages, then the program must be retransmitted for each associated package, with each transmission encrypted with the encryption key corresponding to the particular package. Although the access control is cryptographic, the overhead associated with retransmitting a given program a number of times discourages service providers from placing the same program in a number of packages and thereby limits flexibility in designing packages of programs.

[0008] While such previous systems for encrypting and transmitting programming content have been relatively successful in restricting access to authorized customers, they do not permit a service provider, such as a television network, to offer many different packages containing various numbers of programs to customers, without exceeding the limited secure memory capacity of the set-top terminal. As apparent from the above-described deficiencies with conventional systems for transmitting encrypted programming content, a need exists for a system for transmitting a program encrypted with a unique key, together with the unique key used to encrypt the program. A further need exists for a system that permits a service provider to include a program in a plurality of packages, without requiring the service provider to retransmit the program for each package. Yet another need exists for an access control system that overcomes the secure memory limitations of the set-top terminal without significantly increasing the overhead associated with the transmitted programming content.

SUMMARY OF THE INVENTION

[0009] Generally, encrypted programming content is transmitted by a service provider using a transmitter, or head-end server, to one or more customers. According to one aspect of the invention, the encryption key used to encrypt the program is transmitted to the customer with the programming content. Each customer preferably has a set-top terminal or another mechanism to restrict access to the transmitted multimedia information using decryption keys. According to a further aspect of the invention, the set-top terminal preferably receives one or more package keys, SJ, periodically from the head-end, each corresponding to a package of programs that the customer is entitled to for a given period.

[0010] Each program is preferably encrypted by the head-end server prior to transmission, using a program key, KP, which may be unique to the program. In addition to transmitting the encrypted program, the head-end server preferably transmits header information to the customers, containing a package pair for each package to which the program belongs. A package pair preferably includes an identifier of the package, as well as the program key, KP, encrypted by the corresponding package key, SJ. Thus, in one embodiment, the broadcast of a given program, p, consists of a header portion containing a package pair for each package that the program belongs to, and a program portion containing the program encrypted with the program key, KP. In this manner, if a customer is entitled to a particular program, the set-top terminal will be able to decrypt the encrypted program key, KP, using the appropriate stored package key, SJ, and thereafter use the program key, KP, to decrypt the encrypted program. In various embodiments, the header information can be interleaved with the program portion or transmitted on a separate dedicated control channel.

[0011] A more complete understanding of the present invention, as well as further features and advantages of the present invention, will be obtained by reference to the following detailed description and drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012]

FIG. 1 is a schematic block diagram illustrating a system for transmitting encrypted programming content in accordance with one embodiment of the present invention;

FIG. 2 is an example of the data format of an encrypted program together with a package pair for each package the program belongs to, containing the encryption key used to encrypt the program;

FIG. 3 is a schematic block diagram of an exemplary head-end server of FIG. 1;

FIG. 4 is a schematic block diagram of an exemplary receiver of FIG. 1;

FIG. 5 illustrates a sample table from the program database of FIG. 4;

FIG. 6 illustrates a sample table from the package database of FIG. 4;

FIG. 7 illustrates a sample table from the entitlement database of FIG. 5;

FIG. 8 is a flow chart describing an exemplary transmit process as implemented by the head-end server of FIG.3 ; and

FIGS. 9a and 9b, collectively, are a flowchart describing an exemplary decode process as implemented by the receiver of FIG. 4.

DETAILED DESCRIPTION

[0013] FIG. 1 shows an illustrative network environment for transferring encrypted multimedia information, such as video, audio and data, from a service provider using a transmitter, such as a head-end server 300, to one or more customers having set-top terminals 400-401, such as the set-top terminal 400, over one or more distribution networks 110. As used herein, a set-top terminal includes any mechanism to restrict access to the transmitted multimedia information using decryption keys, including, for example, a computer configuration, as well as telecommunications equipment. It is possible for software executed by the set-top terminal to be downloaded by the service provider. The distribution network 110 can be a wireless broadcast network for distribution of programming content, such as a digital satellite service ("DSS ") or a conventional wired network, such as the cable television network ("CATV"), the Public Switched Telephone Network ("PSTN"), an optical network, a broadband integrated services digital network ("ISDN") or the Internet.

[0014] According to a feature of the present invention, the set-top terminal 400, discussed further below in conjunction with FIG. 4, intermittently receives one or more package keys, SJ, from the head-end server 300, discussed further below in conjunction with FIG. 3, each corresponding to a package that the customer is entitled to for a given time interval, such as a billing period. As used herein, a package is a predefined set of programs, and a given program can belong to one or more packages. A program is any continuous multimedia transmission of a particular length, such as a television episode or a movie. The package keys, SJ, can be downloaded from the head-end server 300 to the set-top tenninal 400 using any suitably secure uni-directional or bi-directional protocol, as would be apparent to a person of ordinary skill.

[0015] As discussed further below, each transmitted program is encrypted by the head-end server 300 using a program key, KP, which may be unique to the program. For a detailed discussion of suitable encryption and security techniques, see B. Schneier, Applied Cryptography (2d ed. 1997), incorporated by reference herein. In addition to transmitting the encrypted program, the head-end server 300 also transmits header information to the set-top terminals 400, containing a package pair for each package to which the program belongs. A package pair includes an identifier of the package, as well as the program key, KP, encrypted by the corresponding package key, SJ.

[0016] Thus, as shown in FIG. 2, the broadcast of a given program, p, consists of a header portion 210 containing a package pair 230 for each package that the program belongs to, and a program portion 220 containing the program encrypted with the program key, KP. In this manner, if a customer is entitled to a particular program, the set-top terminal 400 will be able to decrypt the encrypted program key, KP, using the appropriate stored package key, SJ, and thereafter use the program key, KP, to decrypt the encrypted program.

[0017] FIG. 3 is a block diagram showing the architecture of an illustrative head-end server 300. The head end may be associated with a television network, a cable operator, a digital satellite service operator. or any service provider transmitting encrypted programming content. The head-end server 300 may be embodied, for example, as an RS 6000 server, manufactured by IBM Corp., as modified herein to execute the functions and operations of the present invention. The head-end server 300 preferably includes a processor 310 and related memory, such as a data storage device 320. The processor 310 may be embodied as a single processor, or a number of processors operating in parallel. The data storage device 320 and/or a read only memory (ROM) are operable to store one or more instructions, which the processor 310 is operable to retrieve, interpret and execute. The processor 310 preferably includes a control unit, an arithmetic logic unit (ALU), and a local memory storage device, such as, for example, an instruction cache or a plurality of registers, in a known manner. The control unit is operable to retrieve instructions from the data storage device 320 or ROM. The ALU is operable to perform a plurality of operations needed to carry out instructions. The local memory storage device is operable to provide high-speed storage used for storing temporary results and control information.

[0018] As discussed further below in conjunction with FIGS. 5 and 6, the data storage device 320 preferably includes a program database 500 and a package database 600. The program database 500 preferably stores information on each program, p, which will be transmitted by the head-end server 300, for example, during a given billing period, including the packages the program belongs to and the corresponding program key, KP. The package database 600 preferably stores information on each package offered by the head-end server 300 to customers, including the name of each package and the corresponding package key, SJ.

[0019] In addition, as discussed further below in conjunction with FIG. 8, the data storage device 320 preferably includes a transmit process 800. Generally, the transmit process 800 identifies the program key, KP, of a given program and the packages that the program belongs to, in order to generate the package pairs to be transmitted along with the encrypted program. The communications port 330 connects the head-end server 300 to the distribution network 110, thereby linking the head-end server 300 to each connected receiver, such as the set-top terminal 400 shown in FIG. 1.

[0020] FIG. 4 is a block diagram showing the architecture of an illustrative set-top terminal 400. The set-top terminal 400 may be embodied, for example, as a set-top terminal (STT) associated with a television, such as those commercially available from General Instruments Corp., as modified herein to execute the functions and operations of the present invention. The set-top terminal 400 preferably includes a processor 410 and related memory, such as a data storage device 420, as well as a communication port 430, which operate in a similar manner to the hardware described above in conjunction with FIG. 3.

[0021] As discussed further below in conjunction with FIG. 7, the data storage device 420 preferably includes an entitlement database 700. The entitlement database 700 is preferably stored in a secure portion of the data storage device 420. The entitlement database 700 preferably stores a package identifier and the corresponding package key, SJ, for each package that the customer is entitled to. In addition, as discussed further below in conjunction with FIGS. 9a and 9b, the data storage device 420 preferably includes a decode process 900. Generally, the decode process 900 decrypts programs that a customer is entitled to, by using the corresponding stored package key, SJ, to decrypt the transmitted program key, KP, and then using the program key, KP, to decrypt the program.

[0022] FIG. 5 illustrates an exemplary program database 500 that preferably stores information on each program, p, which will be transmitted by the head-end server 300, for example, during a given billing period, including the packages the program belongs to and the corresponding program key, KP. The program database 500 maintains a plurality of records, such as records 505-520, each associated with a different program. For each program identified by program name in field 525, the program database 500 includes an indication of the corresponding packages to which the program belongs in field 530 and the corresponding program key, KP, in field 535.

[0023] FIG. 6 illustrates an exemplary package database 600 that preferably stores information on each package offered by the head-end server 300 to customers, including the name of each package and the corre-

sponding package key, SJ. The package database 600 maintains a plurality of records. such as records 605-640, each associated with a different package. For each package identified by a package identifier in field 650, the package database 600 includes an indication of the corresponding package name in field 660 and the corresponding package key, SJ, in field 670.

[0024] FIG. 7 illustrates an exemplary entitlement database 700 that preferably stores a package identifier and the corresponding package key, SJ, for each package that the customer is entitled to. The entitlement database 700 maintains a plurality of records, such as records 710-720, each associated with a different entitled package. For each package identified by a package identifier in field 725, the entitlement database 700 includes an indication of the corresponding package key, SJ, in field 735.

[0025] As discussed above, the head-end server 300 preferably executes a transmit process 800, shown in FIG. 8, to identify the program key, KP, of a given program and the packages that the program belongs to, in order to generate the package pairs to be transmitted along with the encrypted program. It is noted that the transmit process 800, other than the actual transmission step, can be executed offline or in real-time. As illustrated in FIG. 8, the transmit process 800 begins the processes embodying the principles of the present invention during step 810 by identifying a program to be transmitted.

[0026] Thereafter, during step 820, the transmit process 800 retrieves the program key, KP, corresponding to the program and the list of packages to which the program belongs from the program database 500. For each package the program belongs to, the transmit process 800 will then retrieve the package identifier and the corresponding package key, SJ, from the package database 600, to generate a package pair to be included in the transmitted header information.

[0027] The program will then be encrypted during step 840 with the program key, KP, retrieved during step 820. Finally, the transmit process 800 will transmit the encrypted program together with the set of package pairs during step 850, before program control terminates during step 860. It is noted that the header information containing the package pairs are preferably transmitted periodically interleaved throughout the transmission of the program information, so that a customer can change channels during a program and be able to obtain the transmitted keys which are required to decrypt the program. The overhead incurred by periodically transmitting the header information should be balanced against the delay a customer will incur after changing a channel until the required decryption keys are obtained. In an alternate embodiment, the header information containing the package pairs can be continuously transmitted on a separate control channel, such as a Barker channel.

[0028] As discussed above, the set-top terminal 400 preferably executes a decode process 900, shown in FIGS. 9a and 9b, to decrypt programs that a customer is entitled to, by using the corresponding stored package key, SJ, to decrypt the transmitted program key, KP, and then using the program key, KP, to decrypt the program. As illustrated in FIG. 9a, the decode process 900 begins the processes embodying the principles of the present invention during step 910, upon receipt of a customer instruction to tune to a particular channel.

[0029] Thereafter, the set-top terminal 400 will tune to the requested channel during step 920 to receive the appropriate signal. The decode process 900 then retrieves the transmitted package pairs during step 930 for the program transmitted on the requested channel. A test is then performed during step 940 to determine if the customer is entitled to a package containing the requested program. For example, the decode process 900 will determine if a package identifier from one of the package pairs retrieved during step 930 matches a package identifier stored in the entitlement database 700.

[0030] If it is determined during step 940 that the customer is not entitled to entitled to a package containing the requested program, then a message is preferably transmitted to the customer during step 950 indicating that the customer is not entitled to view the selected program, before program control terminates during step 960. If, however, it is determined during step 940 that the customer is entitled to a package containing the requested program, then program control proceeds to step 970 (FIG. 9b).

[0031] If the customer is entitled to view the requested program, then the decode process 900 retrieves the package key, SJ, corresponding to the entitled package from the entitlement database 700 during step 970 and then uses the retrieved package key, SJ, during step 980 to decrypt the transmitted program key included in the transmitted header information, or on a separate control channel. Finally, the program itself is decrypted during step 990 using the program key, KP, during step 990, before program control terminates during step 995.

[0032] It is noted that the decode process 900 can wait for the customer to request a particular channel before attempting to obtain the transmitted decryption keys and determine whether the customer is entitled to the requested channel, as described above, or the decode process 900 can alternatively periodically scan all channels to obtain the transmitted package pairs for storage in the data storage device 420 and predetermine the customer's entitlement.

[0033] It is to be understood that the embodiments and variations shown and described herein are merely illustrative of the principles of this invention and that various modifications may be implemented by those skilled in the art without departing from the scope of the invention.

Claims

1. A method of transmitting a plurality of programs having restricted access to an end-user, said method comprising the steps of:

   defining a plurality of packages, each package comprising at least one of said programs;
   providing a package key to said end-user for each package obtained by said end-user;
   encrypting a program to be transmitted to said end-user using a program key; and
   transmitting said encrypted program together with package information for each package said program belongs to, said package information including said program key encrypted with said package key.

2. The method according to claim 1, wherein said package information further comprises an identifier of said associated package.

3. The method according to claim 1 or claim 2, wherein said package information is interleaved with the transmission of said encrypted program.

4. The method according to claim 1 or claim 2, wherein said package information is transmitted on a control channel.

5. A method for decoding an encrypted program associated with a package of programs, said method comprising the steps of:

   receiving said encrypted program together with package information, said package information including a program key encrypted with a package key, said program key being used by a provider of said program to encrypt said program;
   retrieving a package key corresponding to said package;
   decrypting said package information using said retrieved package key to obtain said program key; and
   decrypting said encrypted program using said program key.

6. The method according to claim 5. further comprising the step of receiving one or more package keys from said provider, each package key corresponding to a package of programs a customer is entitled to.

7. The method according to claim 5 or claim 6 wherein said package information further comprises an identifier of said associated package.

8. The method according to any of claims 5 to 7, wherein said package information is interleaved with the transmission of said encrypted program.

9. The method according to any of claims 5 to 7, wherein said package information is transmitted on a control channel.

10. The method according to any of claims 5 to 9, wherein said package information is evaluated upon a request to view said program.

11. The method according to any of claims 5 to 9, wherein said package information is evaluated in advance of a request to view said program.

12. An article of manufacture comprising:

    a computer readable medium having computer readable code means embodied thereon, said computer readable program code means comprising:
    a step to identify one or more packages associated with a program to be transmitted, each of said packages having an associated package key;
    a step to encrypt said program to be transmitted to a plurality of customers using a program key; and
    a step to transmit said encrypted program together with package information for each identified package, said package information including said program key encrypted with said package key.

13. An article of manufacture comprising:

    a computer readable medium having computer readable code means embodied thereon, said computer readable program code means comprising:
    a step to receive an encrypted program together with package information, said package information including a program key encrypted with a package key, said program key being used to encrypt said program;
    a step to retrieve said package key corresponding to a package to which said encrypted program belongs;
    a step to decrypt said package information using said retrieved package key to obtain said program key; and
    a step to decrypt said encrypted program using said program key.

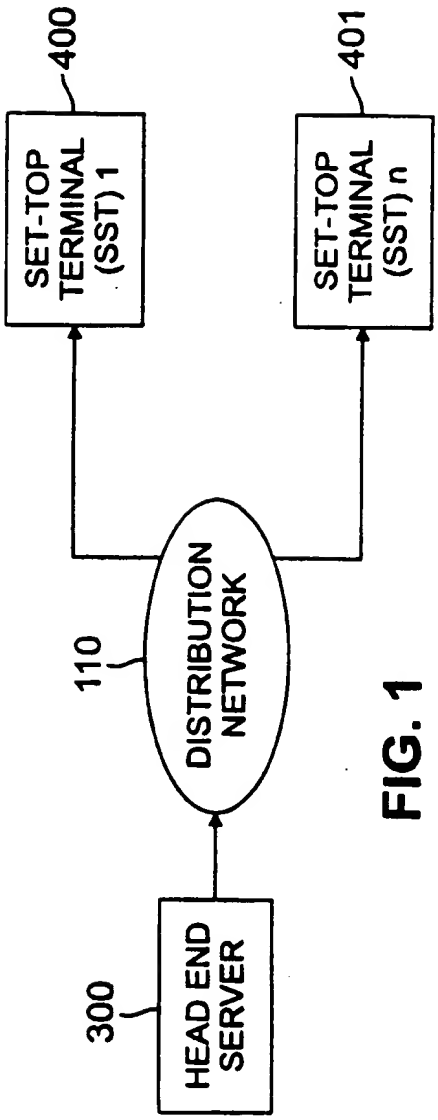
400
SET-TOP TERMINAL (SST) 1
401
SET-TOP TERMINAL (SST) n
110
DISTRIBUTION NETWORK
300
HEAD END SERVER

FIG. 1

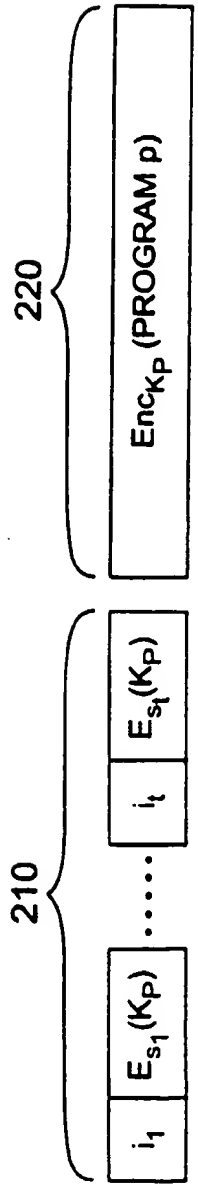
220
Enc_{K_P} (PROGRAM p)
210
i_1
$E_{s_1}(K_P)$
.....
i_t
$E_{s_t}(K_P)$
230

FIG. 2

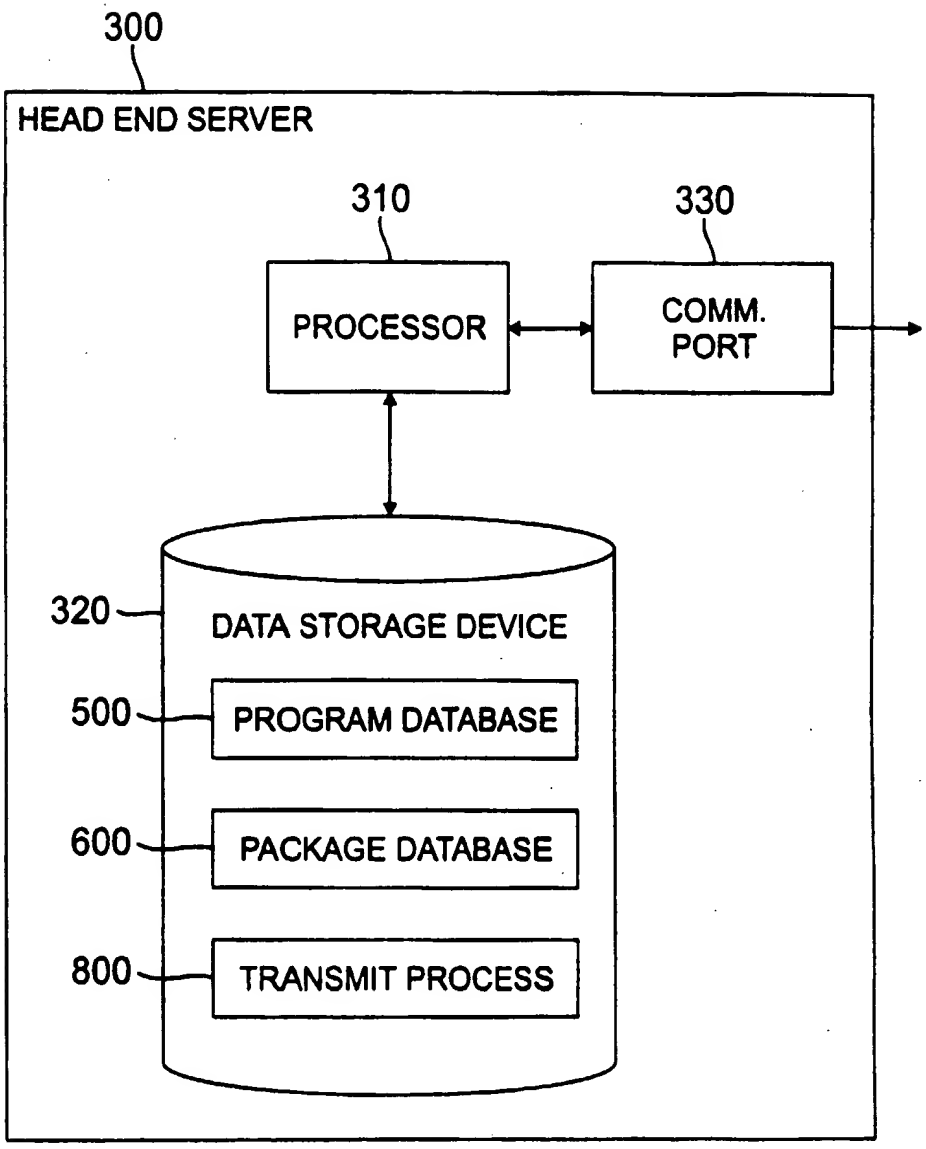
300
HEAD END SERVER
310
330
PROCESSOR
COMM. PORT
320
DATA STORAGE DEVICE
500
PROGRAM DATABASE
600
PACKAGE DATABASE
800
TRANSMIT PROCESS

FIG. 3

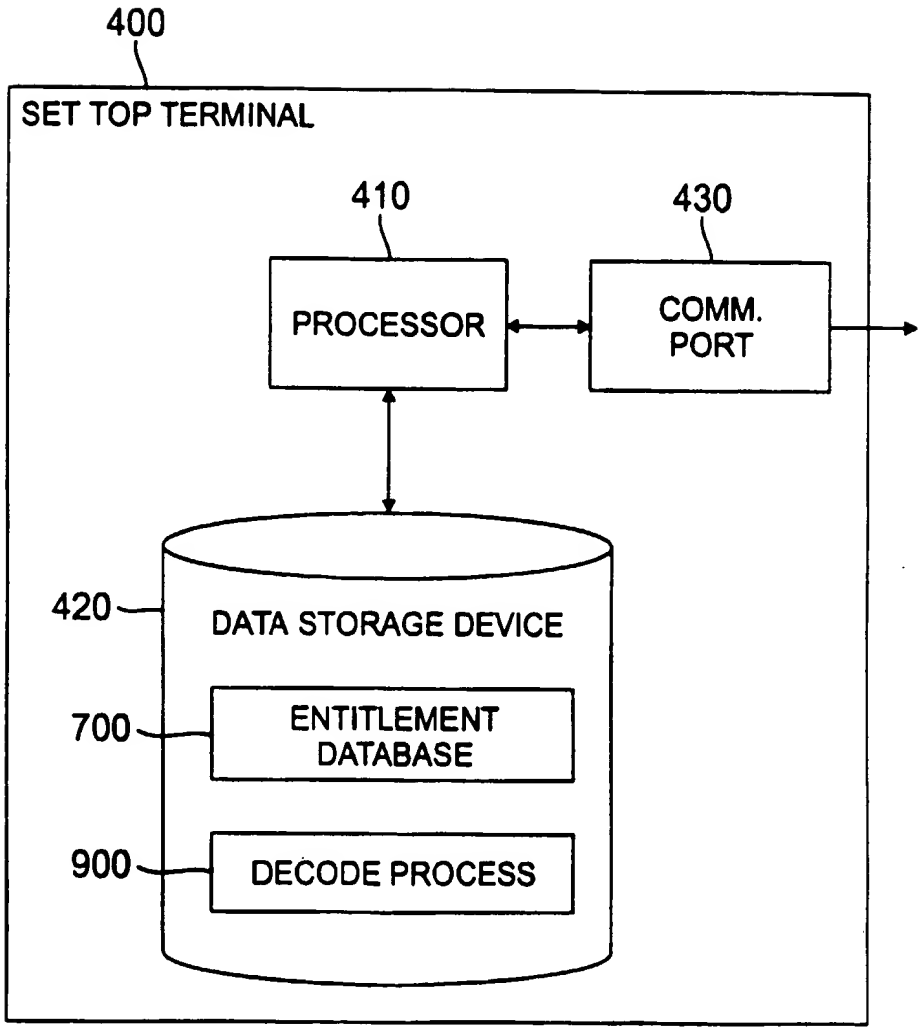
400
SET TOP TERMINAL
410
430
PROCESSOR
COMM. PORT
420
DATA STORAGE DEVICE
700
ENTITLEMENT DATABASE
900
DECODE PROCESS

FIG. 4

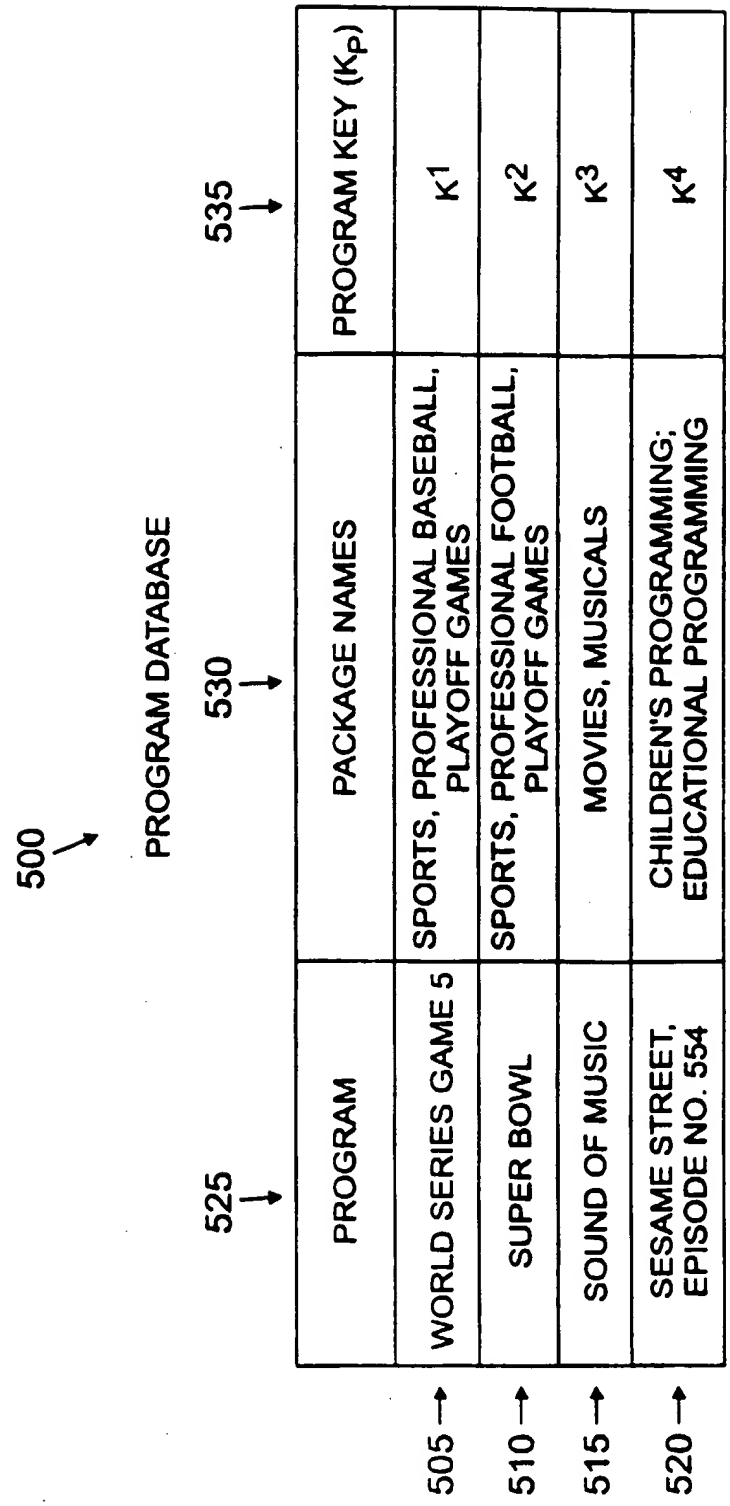
500
PROGRAM DATABASE
525
530
535
PROGRAM
PACKAGE NAMES
PROGRAM KEY (K_P)
505
WORLD SERIES GAME 5
SPORTS, PROFESSIONAL BASEBALL, PLAYOFF GAMES
K^1
510
SUPER BOWL
SPORTS, PROFESSIONAL FOOTBALL, PLAYOFF GAMES
K^2
515
SOUND OF MUSIC
MOVIES, MUSICALS
K^3
520
SESAME STREET, EPISODE NO. 554
CHILDREN'S PROGRAMMING; EDUCATIONAL PROGRAMMING
K^4

FIG. 5

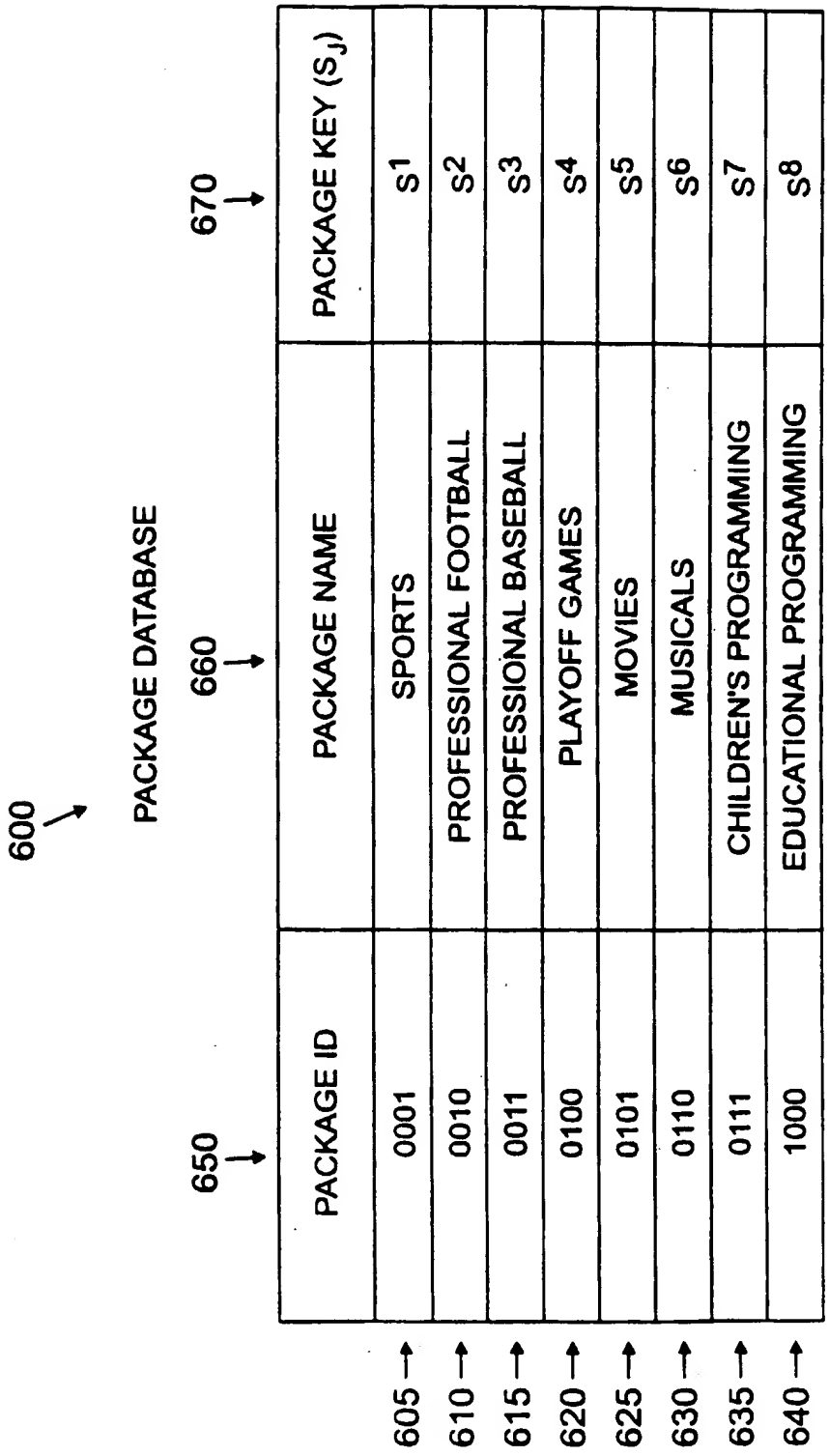
600
PACKAGE DATABASE
650
660
670
PACKAGE ID
PACKAGE NAME
PACKAGE KEY (S_J)
0001
SPORTS
S^1
0010
PROFESSIONAL FOOTBALL
S^2
0011
PROFESSIONAL BASEBALL
S^3
0100
PLAYOFF GAMES
S^4
0101
MOVIES
S^5
0110
MUSICALS
S^6
0111
CHILDREN'S PROGRAMMING
S^7
1000
EDUCATIONAL PROGRAMMING
S^8
605
610
615
620
625
630
635
640

FIG. 6

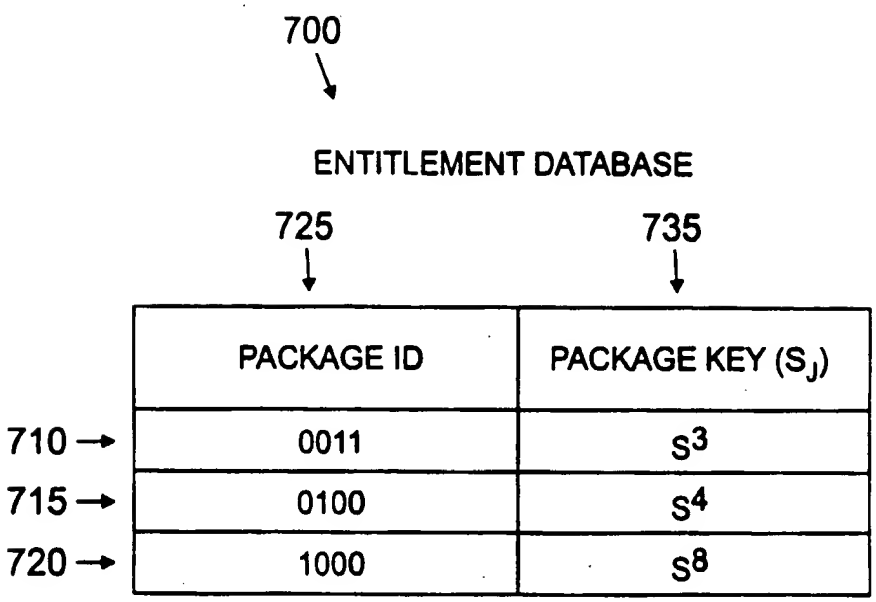
700
ENTITLEMENT DATABASE
725
735
PACKAGE ID
PACKAGE KEY (S_J)
710
0011
S^3
715
0100
S^4
720
1000
S^8

FIG. 7

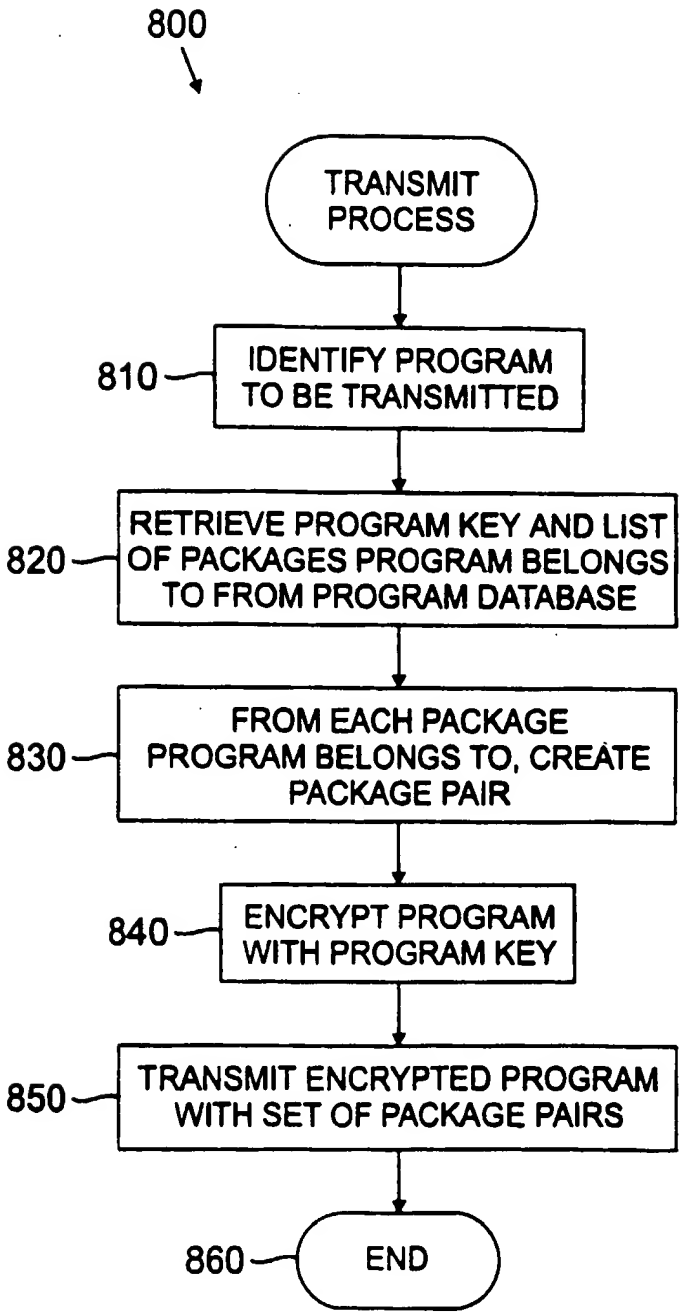
800
TRANSMIT PROCESS
810
IDENTIFY PROGRAM TO BE TRANSMITTED
820
RETRIEVE PROGRAM KEY AND LIST OF PACKAGES PROGRAM BELONGS TO FROM PROGRAM DATABASE
830
FROM EACH PACKAGE PROGRAM BELONGS TO, CREATE PACKAGE PAIR
840
ENCRYPT PROGRAM WITH PROGRAM KEY
850
TRANSMIT ENCRYPTED PROGRAM WITH SET OF PACKAGE PAIRS
860
END

FIG. 8

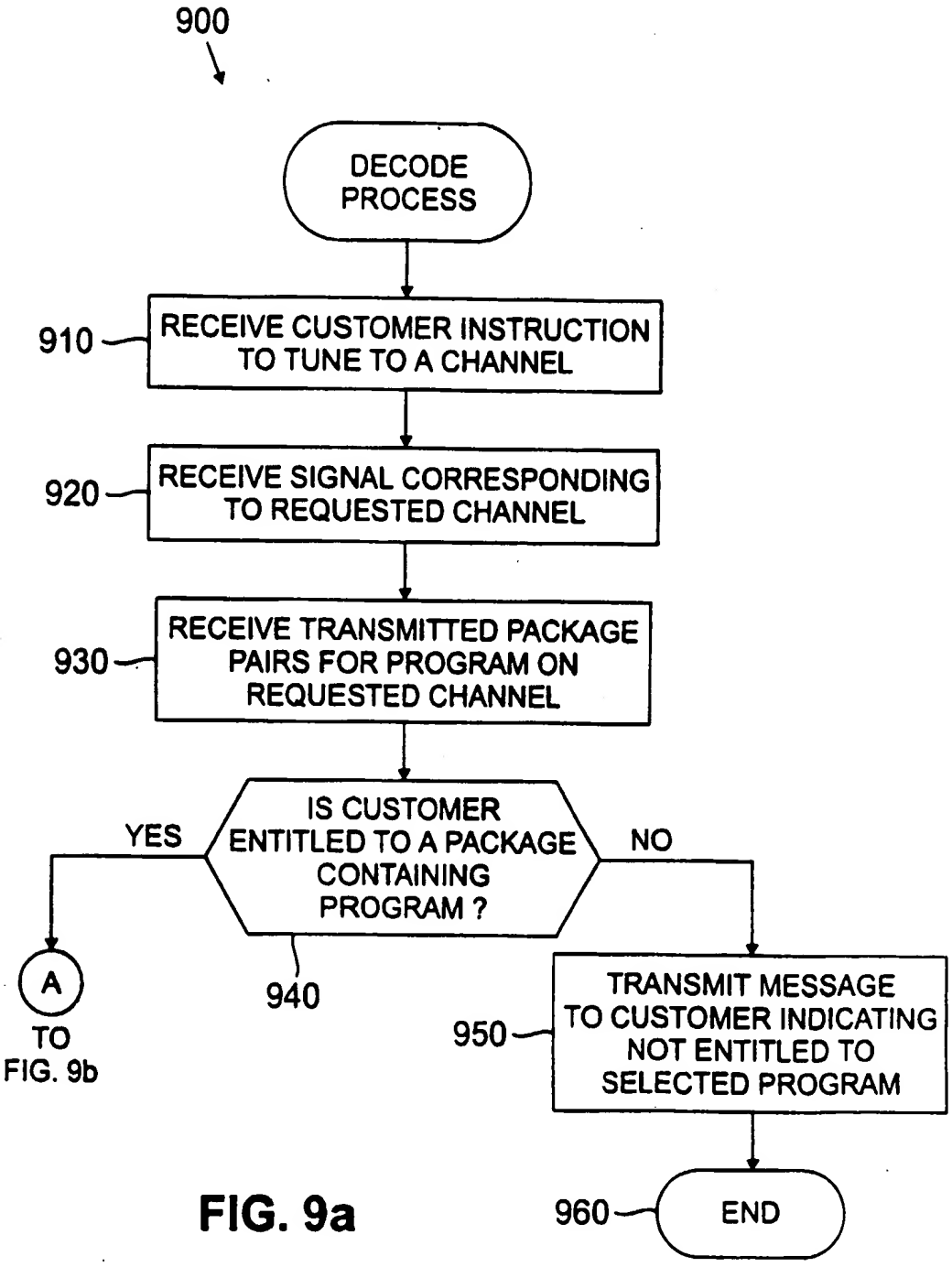
900
DECODE PROCESS
910
RECEIVE CUSTOMER INSTRUCTION TO TUNE TO A CHANNEL
920
RECEIVE SIGNAL CORRESPONDING TO REQUESTED CHANNEL
930
RECEIVE TRANSMITTED PACKAGE PAIRS FOR PROGRAM ON REQUESTED CHANNEL
IS CUSTOMER ENTITLED TO A PACKAGE CONTAINING PROGRAM ?
YES
NO
940
A
TO FIG. 9b
950
TRANSMIT MESSAGE TO CUSTOMER INDICATING NOT ENTITLED TO SELECTED PROGRAM
960
END

FIG. 9a

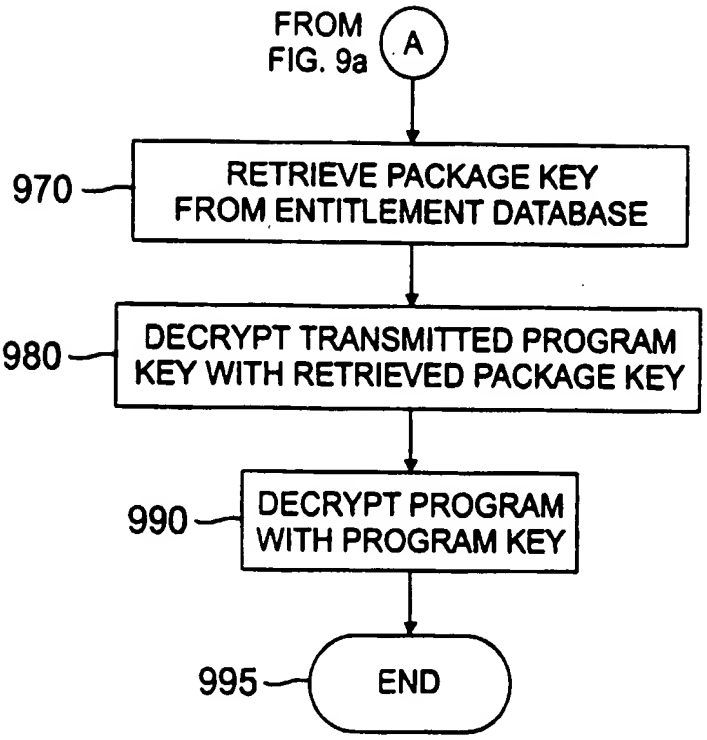
FROM FIG. 9a
A
970
RETRIEVE PACKAGE KEY FROM ENTITLEMENT DATABASE
980
DECRYPT TRANSMITTED PROGRAM KEY WITH RETRIEVED PACKAGE KEY
990
DECRYPT PROGRAM WITH PROGRAM KEY
995
END

FIG. 9b